MARCH 2013

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special **REPORT**

Test Results for Digital Data Acquisition Tool: X-Ways Forensics 14.8

nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Eric H. Holder, Jr.
Attorney General

Mary Lou Leary
Acting Assistant Attorney General

Greg Ridgeway
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

NIJ

MARCH 2013

Test Results for Digital Data Acquisition Tool: X-Ways Forensics 14.8

NCJ 236224

NIJ

Greg Ridgeway
Acting Director, National Institute of Justice

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003–IJ–R–029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

March 2013

Test Results for Digital Data Acquisition Tool:
X-Ways Forensics 14.8

National Institute of
Standards and Technology
U.S. Department of Commerce

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's Law Enforcement Standards Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, the U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service (USSS). The objective of the CFTT program is to provide measurable assurance to practitioners, researchers and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensic tools is based on well-recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the CFTT Web site (http://www.cftt.nist.gov/) for review and comment by the computer forensics community.

This document reports the results from testing X-Ways Forensics, Version 14.8, against the *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0,* available at the CFTT Web site (http://www.cftt.nist.gov/DA-ATP-pc-01.pdf).

Test results from other tools and the CFTT tool methodology can be found on NIJ's CFTT Web page, http://www.nij.gov/nij/topics/forensics/evidence/digital/standards/cftt.htm.

How to Read This Report

This report is divided into five sections. The first section is a summary of the results from the test runs and is sufficient for most readers to assess the suitability of the tool for the intended use. The remaining sections of the report describe how the tests were conducted, discuss any anomalies that were encountered and provide documentation of test case run details that support the report summary. Section 2 gives justification for the selection of test cases from the set of possible cases defined in the test plan for Digital Data Acquisition tools. The test cases are selected, in general, based on features offered by the tool. Section 3 describes in more depth any anomalies summarized in the first section. Section 4 lists hardware and software used to run the test cases, with links to additional information about the items used. Section 5 contains a description of each test case run. The description of each test run lists all test assertions used in the test case, the expected

result and the actual result. For more information pertaining to the features and usage of X-Ways Forensics, see the vendor Web site (http://www.x-ways.com).

Test Results for Digital Data Acquisition Tool

Tool Tested:	X-Ways Forensics
Version:	14.8
Run Environments:	Windows: 2000 & XP
Supplier:	X-Ways Software Technology AG
Address:	X-Ways AG Agrippastr. 37-39 50676 Cologne Germany
Tel:	+49 221-420 486 5
Fax:	+49 3212-123 2029
Email:	mail@x-ways.com
WWW:	http://www.x-ways.com

1 Results Summary

The tool acquired source drives completely and accurately except for the cases where source drives containing faulty sectors were imaged, a logical NTFS partition was imaged, or a source drive containing hidden sectors, a *Host Protected Area* (HPA) or *Device Configuration Overlay* (DCO), was imaged. The tool restored image files and created clones accurately except for clone or restore operations on certain partitions and removable media where small changes to file system metadata were observed. The following anomalies were observed:

- Some readable sectors may be intentionally skipped, controlled by a parameter setting, to improve performance during acquisition of a drive with faulty sectors (DA-09-FW, DA-09-FW-XP and DA-09-USB).
- Eight unused sectors at the end of a partition containing an NT file system are not acquired (DA-07-NTFS). This is because the tool user selected acquiring the logical drive rather than the physical drive. If the physical drive is selected, all sectors of the partition should be acquired. This is not an issue with the tool; this result is noted to make the reader aware of the differences between choosing a logical vs. a physical acquisition.
- The tool does not acquire any sectors hidden by an HPA or a DCO. However, a separate tool, X-Ways Replica, can be used to remove an HPA or a DCO to make hidden sectors visible and then acquire the formerly hidden sectors (DA-08-ATA28, DA-08-ATA48 and DA-08-DCO).
- Small changes may be made by the operating system to file system metadata when cloning or restoring the image of a FAT32 or NTFS logical drive (DA-02-CF, DA-02-F32, DA-02-F32X, DA-14-CF, DA-14-F32, DA-14-F32X and DA-14-NTFS). The tool has no control over these changes.

- Only the first 268,435,456 sectors (128GB) of a drive larger than 128GB are acquired if the tool is executed in the Windows 2000 environment (DA-08-DCO). This is because of the limitations of Windows 2000 to handle drives requiring 48bit addressing. This is not an issue with the tool; this result is noted to make the reader aware of the consequences of operating system selection.

2 Test Case Selection

Test cases used to test disk imaging tools are defined in *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*. To test a tool, test cases are selected from the *Test Plan* document based on the features offered by the tool. Not all test cases or test assertions are appropriate for all tools. There is a core set of base cases (DA-06, DA-07 and DA-08) that are executed for every tool tested. Tool features guide the selection of additional test cases. If a given tool implements a given feature, then the test cases linked to that feature are run. Table 1 lists the features selected for testing and the linked test cases selected for execution. Table 2 lists the features not selected for testing and the test cases not executed.

Table 1 Selected Test Cases

Supported Optional Feature	Cases Selected for Execution
Base Cases	06, 07 & 08
Read error during acquisition	09
Create a clone from an image file	14 & 17
Destination Device Switching	13
Create a clone during acquisition	01
Create an unaligned clone from a digital source	02
Create a truncated clone from a physical device	04

Table 2 Omitted Test Cases

Unsupported Optional Feature	Cases Omitted (Not Executed)
Create cylinder aligned clones	03, 15, 21 & 23
Convert an image file from one format to another	26
Insufficient space for image file	12
Alternate image formats	10
Device I/O error generator available	05, 11 & 18
Fill excess sectors on a clone device	20, 21, 22 & 23
Create a clone from a subset of an image file	16
Fill excess sectors on a clone acquisition	19
Detect a corrupted (or changed) image file	24 & 25

Some test cases have variant forms to accommodate parameters within test assertions. These variant forms are designed to cover parameters that can vary within the test assertions. These variations cover the acquisition interface to the source drive (SRC-AI),

the type of digital source (DS) object acquired, the execution environment (XE) and the way that sectors are hidden on a drive. Additional parameters that were varied between test cases and test case variations were types of hash algorithm calculated, image file segment size, the use of a hardware write blocker and the type of hardware write blocker used.

The following source access interfaces were tested: ATA28, ATA48, SATA28, SATA48, SCSI, FW, and USB. These are noted as variations on test cases DA-01, DA-06, DA-08 and DA-14.

The following digital sources were tested: partitions (FAT12, FAT16, FAT32, FAT32X, NTFS), compact flash (CF) and thumb drive (Thumb). There are two FAT 32 variations testing acquisition of both FAT 32 partition codes 0x0B (FAT32) and 0x0C (FAT32X). These digital source types are noted as variations on test cases DA-02 and DA-07.

Hardware write blockers were used in certain variations of the DA-01, DA-02, DA-07, DA-08 and DA-09 test cases.

3 Results by Test Assertion

A test assertion is a verifiable statement about a single condition after an action is performed by the tool under test. A test case usually checks a group of assertions after the action of a single execution of the tool under test. Test assertions are defined and linked to test cases in *Digital Data Acquisition Tool Assertions and Test Plan Version 1.0*. Table 3 summarizes the test results for all the test cases by assertion. The column labeled **Assertions Tested** gives the text of each assertion. The column labeled **Tests** gives the number of test cases that use the given assertion. The column labeled **Anomaly** gives the section number in this report where any observed anomalies are discussed.

See Section 2 for a discussion of source access interface, execution environment and digital source.

Table 3 Assertions Tested

Assertions Tested	Tests	Anomaly
AM-01 The tool uses access interface SRC-AI to access the digital source.	38	
AM-02 The tool acquires digital source DS.	38	
AM-03 The tool executes in execution environment XE.	53	
AM-04 If clone creation is specified, the tool creates a clone of the digital source.	13	
AM-05 If image file creation is specified, the tool creates an image file on file system type FS.	25	
AM-06 All visible sectors are acquired from the digital source.	38	3.3, 3.4, 3.5
AM-07 All hidden sectors are acquired from the digital source.	3	3.2

Assertions Tested	Tests	Anomaly
AM-08 All sectors acquired from the digital source are acquired accurately.	38	3.1
AM-09 If unresolved errors occur while reading from the selected digital source, the tool notifies the user of the error type and location within the digital source.	5	
AM-10 If unresolved errors occur while reading from the selected digital source, the tool uses a benign fill in the destination object in place of the inaccessible data.	5	
AO-01 If the tool creates an image file, the data represented by the image file is the same as the data acquired by the tool.	25	
AO-04 If the tool is creating an image file and there is insufficient space on the image destination device to contain the image file, the tool shall notify the user.	1	
AO-05 If the tool creates a multi-file image of a requested size, then all the individual files shall be no larger than the requested size.	25	
AO-10 If there is insufficient space to contain all files of a multi-file image, and if destination device switching is supported, the image is continued on another device.	1	
AO-11 If requested, a clone is created during an acquisition of a digital source.	13	
AO-12 If requested, a clone is created from an image file.	15	
AO-13 A clone is created using access interface DST-AI to write to the clone device.	28	
AO-14 If an unaligned clone is created, each sector written to the clone is accurately written to the same disk address on the clone that the sector occupied on the digital source.	27	3.1
AO-17 If requested, any excess sectors on a clone destination device are not modified.	12	
AO-19 If there is insufficient space to create a complete clone, a truncated clone is created using all available sectors of the clone device.	2	
AO-20 If a truncated clone is created, the tool notifies the user.	2	
AO-23 If the tool logs any log significant information, the information is accurately recorded in the log file.	53	
AO-24 If the tool executes in a forensically safe execution environment, the digital source is unchanged by the acquisition process.	38	

Table 4 Assertions Not Tested

Assertions Not Tested
AO-02 If an image file format is specified, the tool creates an image file in the specified format.
AO-03 If there is an error while writing the image file, the tool notifies the user.

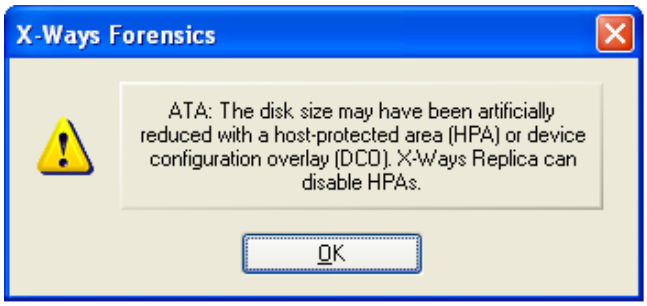
Assertions Not Tested
AO-06 If the tool performs an image file integrity check on an image file that has not been changed since the file was created, the tool shall notify the user that the image file has not been changed.
AO-07 If the tool performs an image file integrity check on an image file that has been changed since the file was created, the tool shall notify the user that the image file has been changed.
AO-08 If the tool performs an image file integrity check on an image file that has been changed since the file was created, the tool shall notify the user of the affected locations.
AO-09 If the tool converts a source image file from one format to a target image file in another format, the acquired data represented in the target image file is the same as the acquired data in the source image file.
AO-15 If an aligned clone is created, each sector within a contiguous span of sectors from the source is accurately written to the same disk address on the clone device relative to the start of the span as the sector occupied on the original digital source. A span of sectors is defined to be either a mountable partition or a contiguous sequence of sectors not part of a mountable partition. Extended partitions, which may contain both mountable partitions and unallocated sectors, are not mountable partitions.
AO-16 If a subset of an image or acquisition is specified, all the subset is cloned.
AO-18 If requested, a benign fill is written to excess sectors of a clone.
AO-21 If there is a write error during clone creation, the tool notifies the user.
AO-22 If requested, the tool calculates block hashes for a specified block size during an acquisition for each block acquired from the digital source.

3.1 Metadata Changes During Restore or Clone

Small changes to file system metadata may occur when creating a clone or restoring the image of a FAT32 or NTFS logical drive. For FAT32 file systems, there are usually no more than three sectors with changes. The more intricate NTFS may have more than 200 sectors of metadata with at least one byte changed (DA-02-CF, DA-02-F32, DA-02-F32X, DA-14-CF, DA-14-F32, DA-14-F32X and DA-14-NTFS). These changes are made by the operating system. Sometimes the changes can be prevented by removing the device without following the normal shutdown procedure.

3.2 Acquisition of HPA and DCO

The tool does not remove an HPA or a DCO. The tool did not acquire sectors hidden by an HPA, or a DCO in test case DA-08 variations DA-08-DCO, DA-08-ATA28 and DA-08-ATA48. A separate tool, X-ways Replica, can be used to remove an HPA. The tool displays the following pop-up window if an HPA or a DCO is detected:



3.3 Logical Acquisition of NTFS Partition

Eight unused sectors at the end of a partition containing an NTFS file system are not acquired (DA-07-NTFS). The partition has 27,744,192 sectors but the tool acquires only 27,744,184 sectors, skipping the last eight sectors. However, the last eight sectors of an NT file system are not used to contain any user data. The eight sectors are omitted because the tool user selected acquiring the logical drive rather than the physical drive. If the physical drive is selected, all sectors of the partition should be acquired. This is not an issue with the tool; this result is noted to make the reader aware of the differences between choosing a logical vs. a physical acquisition.

3.4 Acquisition of 48bit Address Drive From Windows 2000

Only the first 268,435,456 sectors of a drive that requires 48bit addressing (i.e., larger than 128GB) are acquired if the tool is executed in the Windows 2000 environment (DA-08-DCO). Windows 2000 should not be used to acquire drives larger than 128GB.

3.5 Acquisition of Faulty Sectors

The tool allows the specification of a number of sectors to skip when a faulty sector is encountered. This feature improves tool performance, but some readable sectors are not acquired when the skip feature is used (DA-09-FW, DA-09-FW-XP and DA-09-USB).

4 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the test computers available for testing, using the support software, and notes on other test hardware.

4.1 Test Computers

Three test computers were used.

Freddy, **Frank** and **Joe** have the following configuration:

Intel Desktop Motherboard D865GB/D865PERC (with ATA-6 IDE on board controller)
BIOS Version BF86510A.86A.0053.P13
Adaptec SCSI BIOS V3.10.0
Intel® Pentium™ 4 CPU 3.4Ghz
2577972KB RAM

SONY DVD RW DRU-530A, ATAPI CD/DVD-ROM drive
1.44 MB floppy drive
Two slots for removable IDE hard disk drives
Two slots for removable SATA hard disk drives
Two slots for removable SCSI hard disk drives

4.2 Support Software

A package of programs to support test analysis, FS-TST Release 2.0, was used. The software can be obtained from http://www.cftt.nist.gov/diskimaging/fs-tst20.zip.

4.3 Test Drive Creation

There are three ways that a hard drive may be used in a tool test case: as a source drive that is imaged by the tool, as a media drive that contains image files created by the tool under test, or as a destination drive on which the tool under test creates a clone of the source drive. In addition to the operating system drive formatting tools, some tools (**diskwipe** and **diskhash**) from the FS-TST package are used to set up test drives.

To set up a media drive, the drive is formatted with one of the supported file systems. A media drive may be used in several test cases.

The setup of most source drives follows the same general procedure, but there are several steps that may be varied depending on the needs of the test case.

1. The drive is filled with known data by the **diskwipe** program from FS-TST. The **diskwipe** program writes the sector address to each sector in both C/H/S and LBA format. The remainder of the sector bytes is set to a constant fill value unique for each drive. The fill value is noted in the **diskwipe** tool log file.
2. The drive may be formatted with partitions as required for the test case.
3. An operating system may optionally be installed.
4. A set of reference hashes is created by the FS-TST **diskhash** tool. These include both SHA1 and MD5 hashes. In addition to full drive hashes, hashes of each partition may also be computed.
5. If the drive is intended for hidden area tests (DA-08), an HPA, a DCO or both may be created. The **diskhash** tool is then used to calculate reference hashes of just the visible sectors of the drive.

The source drives for DA-09 are created such that there is a consistent set of faulty sectors on the drive. Each of these source drives is initialized with **diskwipe** and then their faulty sectors are activated. For each of these source drives, a second drive of the same size with the same content as the faulty sector drive but with no faulty sectors serves as a reference drive for images made from the faulty drive.

To set up a destination drive, the drive is filled with known data by the **diskwipe** program from FS-TST. Partitions may be created if the test case involves restoring from the image of a logical acquire.

4.4 Test Drive Analysis

For test cases that create a clone of a physical device (e.g., DA-01 and DA-04), the destination drive is compared to the source drive with the **diskcmp** program from the FS-TST package. For test cases that create a clone of a logical device (i.e., a partition, e.g., DA-02 and DA-20), the destination partition is compared to the source partition with the **partcmp** program. For a destination created from an image file (e.g., DA-14), the destination is compared, using either **diskcmp** (for physical device clones) or **partcmp** (for partition clones), to the source that was acquired to create the image file. Both **diskcmp** and **partcmp** note differences between the source and destination.

If the destination is larger than the source, then the excess destination sectors are categorized as either, undisturbed (still containing the fill pattern written by **diskwipe**), zero filled or changed to something else. A tool may provide a feature to wipe the excess sectors. For an FAT partition, the **diskcmp** and **partcmp** programs report the final state of the excess sectors. For an NTFS partition, metadata may be written to the excess sectors, overwriting the fill values placed by **diskwipe**. A special procedure is used to determine the state of excess sectors after restoring an NTFS partition, such as test case DA-14-NTFS. A destination drive is first pattern-filled with **diskwipe**, then, before restoring the partition, a hash is computed over the excess sectors on the destination. After the tool is used to restore the partition, another hash is computed over the excess sectors of the destination. If the two hashes match then none of the excess sectors have been changed by the tool.

For test case DA-09, imaging a drive with known faulty sectors, the program **anabad** is used to compare the faulty sector reference drive to a cloned version of the faulty sector drive.

For test cases such as DA-06 and DA-07, any acquisition hash computed by the tool under test is compared to the reference hash of the source to check that the source is completely and accurately acquired.

4.5 Comments on Test Drives

The testing uses several test drives from a variety of vendors. The drives are identified by an external label that consists of a 2-digit hexadecimal value and an optional tag (e.g., 25-SATA). The combination of hex value and tag serves as a unique identifier for each drive. The two digit hex value is used by the FS-TST **diskwipe** program as a sector fill value. The FS-TST compare tools, **diskcmp** and **partcmp**, count sectors that are filled with the source and destination fill values on a destination that is larger than the original source.

Table 5 lists the source test drives used. The models and serial numbers are listed as returned by the ATA IDENTIFY DEVICE command.

Table 5 Test Drives

Drive	Model	Serial #	Size (Sectors)
01-IDE	WDC WD400BB-00JHC0	WD-WMAMC7417100	78165360